Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

10 Questions The SEC Will Probably Ask Google: Part 1

By **John Reed Stark** (October 9, 2018, 6:30 PM EDT)

John Reed Stark

Google has a problem and, having served for over 11 years as chief of the U.S. Securities and Exchange Commission's Office of Internet Enforcement, my guess is that the SEC is probably investigating.

On Oct. 8, 2018, Google announced that it will close most of its failing social media platform, Google+, and implement several new privacy measures because of a previously undisclosed software bug relating to its Google+ application programming interface. Google created the API to help app developers access an array of profile and contact information about the people who sign up to use their apps, as well as the people they are connected to on Google+.

Google also mentioned that up to 500,000 Google+ users potentially had their personal data exposed. In addition, Google reported that up to 438 applications may have used the defective Google+ API, which makes estimations of impacted individuals difficult to ascertain.

Meanwhile, the Wall Street Journal and the Washington Post are reporting that Google hid the Google+ API defect from shareholders and others for fear of regulatory examination, congressional inquiry and other negative ramifications.

What a mess. Let the onslaught of scrutiny begin, which in my opinion will undoubtedly include an investigation by the SEC, the federal regulator tasked with policing the disclosures to shareholders by public companies like Google.

But what precisely will the SEC want to know? Assuming I am right about an ongoing SEC investigation, this two-part series presents 10 questions SEC enforcement staff will be posing to Google executives and others in connection with an investigation of Google's public disclosures of the Google+ API defect.

Part one of this series discusses: (1) some critical background concerning SEC disclosure requirements of cybersecurity risks and events; and (2) the first five of 10 general questions that Google will likely have to answer if the SEC investigates.

Part two will discuss: (1) the second five of 10 general questions that Google will likely have to answer if the SEC investigates; and (2) some final thoughts looking ahead for Google and their current predicament.

Some Background: After 2018 SEC Cybersecurity Disclosure Guidance

On Feb. 20, 2018, the SEC issued interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

The 2018 guidance offers the SEC's views about public companies' disclosure obligations under existing law with respect to matters involving cybersecurity risk and incidents. It also addresses the importance of cybersecurity policies and procedures and the application of disclosure controls

the importance of cybersecurity policies and procedures and the application of disclosure controls and processes, insider trading prohibitions, and Regulation FD and selective disclosure prohibitions in the cybersecurity context.

The 2018 SEC guidance serves as a follow-up to the Oct. 13, 2011, SEC Division of Corporation Finance staff guidance, which also pertained exclusively to the cybersecurity-related disclosure obligations of public companies.

The fact that the 2011 guidance was published by the staff while the 2018 guidance was adopted by the commission itself, though indicative of the gravity of the issue of the SEC and cyber incident disclosure, makes little actual difference for practitioners. Whether guidance emanates from the SEC staff or from the SEC itself, it should be taken with the same high level of significance and attentiveness.

Along those lines, much of the 2018 SEC guidance tracks the 2011 SEC CF guidance, retaining a focus on "material" cyber risks and incidents and expanding upon its predecessor while also reinforcing the SEC's expectations about cyber disclosure. But if the 2011 SEC CF guidance was a wake-up call for public companies, the 2018 guidance was a resounding fire alarm — and is a must-read for any C-suite executive at a public company.

In short, the 2018 SEC guidance:

- Stresses the need for public companies to put into practice disclosure controls and procedures designed to escalate cybersecurity risks and incidents to the right C-suite executives;
- Emphasizes the urgency for public companies to make appropriate disclosure to investors; and
- Articulates the SEC's growing concerns about unlawful trading involving data security incidents.

The 2018 SEC guidance also serves as a stark reminder for public companies that disclosures relating to data security events present an array of regulatory and litigation issues and has quickly evolved into an increasingly specialized area of securities regulation.

Before 2018 SEC Cyber Disclosure Guidance

On Oct. 13, 2011, the SEC released the 2011 SEC CF guidance, its first staff guidance pertaining exclusively to the cybersecurity-related disclosure obligations of public companies. With the 2011 guidance, the SEC officially (and quite noticeably) added cybersecurity into the mix of disclosure by putting every public company on notice that cyberattacks and cybersecurity vulnerabilities fell squarely within a public company's reporting responsibilities.

The 2011 SEC CF guidance covered a public company's reporting responsibilities both just after a cyberattack as a "material" event, and before as a "risk factor." In their essence, these notions clarified the SEC's long-standing requirement that public companies report "material" events to their shareholders. What precisely renders an event material has plagued securities lawyers for years and has been the subject of countless judicial decisions, SEC enforcement actions, law review articles, law firm guidance and the like — but can be effectively summed up as any important development or event that "a reasonable investor would consider important to an investment decision."

Prior to the 2011 SEC CF guidance, publicly traded companies were not necessarily required to report in their SEC filings if a data security incident had occurred or if they had fixed the problem. After the 2011 guidance, however, publicly traded companies were more compelled to acknowledge cyberattacks and other data security incidents to regulators, and explain the measures they planned to take to close their cybersecurity gaps.

With respect to the aftermath of a cyberattack, the 2011 SEC CF guidance discussed the myriad

ways a cyberattack can impact the operations of a public company. Next the guidance set forth the various reporting sections of typical SEC filings that could warrant mention of the cyberattack, including risk factors; management's discussion and analysis of financial condition and results of operations; description of business, legal proceedings, financial statement disclosures; and disclosure controls and procedures.

With respect to the mere possibility of a cyberattack, the 2011 SEC CF Guidance noted that companies should also "consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption."

Even though the SEC staff might have viewed the 2011 guidance as simply a reiteration of previously existing requirements, there remained little doubt at the time of its publication that the guidance imposed an arguably unprecedented and certainly significant obligation upon public companies.

Against the backdrop of the 2011 CF guidance and the 2018 SEC guidance, below are the questions Google should expect from SEC enforcement staff.

1. Was Google's internal investigation of the Google+ API vulnerability a fulsome and robust process of neutrality, objectivity, transparency and candor?

When it comes to data security incidents, one option for Google is to investigate the problem itself — get to the bottom of it, improve security practices, policies and procedures and move forward with better, stronger and more robust security. This seems to have been Google's approach — and it may have very well succeeded.

However, there is a far more effective, more rewarding and more cost-effective option, which SEC enforcement staff has come to respect and appreciate. Whether it is British Petroleum struggling to handle the aftermath of an oil refinery explosion killing 15 Alaskan workers, Wells Fargo adjusting its operations after a massive company fraud committed by 5,300 employees against over 2 million customer accounts, or any company experiencing a threat to its customers, the same lesson always rings true. Confront the issue head-on with independence, transparency and integrity.

For starters, strong leaders seek answers from independent and neutral sources of information when responding to data security incidents. Google's leaders should:

- Engage a former law enforcement agent or prosecutor from an independent and neutral law firm or consulting firm (preferably never engaged before) to conduct an investigation and report its findings to the board;
- Direct the law firm to engage an independent digital forensics firm to examine the Google+ API issue;
- Report the investigation's progress to shareholders, regulators and other constituencies and fiduciaries every step of the way; and
- Disclose the details of the findings to those users impacted.

Instead of trying to characterize an incident, effective leaders begin with these three steps, which evidence strong corporate ethics, fierce customer dedication and steadfast corporate governance.

Next is to anoint someone from the engaged outside investigative team to serve as the face of the response. This person should have impeccable credentials and the kind of gravitas that customers, shareholders and other important members of the public will trust and respect.

By navigating problems with integrity and transparency, Google can shift the tides in its favor, seizing the opportunity to reinforce strong business ethics, renewed customer dedication and

seizing the opportunity to reinforce strong business ethics, renewed customer dedication and steadfast corporate governance.

But Google's announcement makes no mention of any independent investigation. Rather Google's announcement focuses on findings and conclusions rendered by its own "Privacy & Data Protection Office," a council of top Google product executives who oversee key decisions relating to privacy.

C-suite executives and boards of directors are not politicians and do not have the luxury of conducting potentially self-serving investigations and offering sanitized reports and findings; they have fiduciary obligations to shareholders and others to seek the truth and they should do so with independency, neutrality, transparency and candor. Otherwise, any formal findings can lack credibility and integrity, and no one, including the SEC enforcement staff, will take the investigative and remedial effort seriously.

2. What did the Google board know, and when?

The 2018 SEC guidance for public companies on cybersecurity-related disclosures garnered a great deal of attention for what it says about the threat and risk that cybersecurity presents for public companies — large and small. With cyber incidents capturing headlines around the world with increasing frequency, businesses and regulators have come to recognize that cyber incidents are not a passing trend, but rather in our digitally connected economy, an embedded risk that is here to stay. Indeed, these cybersecurity risks represent a mounting threat to businesses — risks that can never be completely eliminated.

Much of the published commentary concerning the 2018 SEC guidance focused on the technical aspects of the SEC's instructions regarding the need for additional disclosure in a company's periodic filings and the SEC's updated views on the timing of cyber-related disclosures and what that means for insider trading windows. However, the 2018 guidance also says a lot about the SEC's expectations of boards with respect to data security incidents, including disclosure-related responsibilities.

The SEC's views on the role of the board have evolved over the past few years, culminating with the release of the 2018 guidance, which likely prompted many corporate boards to take tangible steps to translate their general awareness and high-level concerns around cybersecurity risks into specific behaviors and precise actions that are identifiable, capable of being readily implemented and heavily documented.

The comments contained in the 2018 guidance evidence the SEC's strong views regarding the board's essential role in this emerging area of enterprise risk, and remove any doubt that for those who serve as corporate directors, "cybersecurity" can no longer be just a buzz word or a simple talking point. While many board members characterize cybersecurity risks as "an existential threat," few, if any, have taken the time to go beyond attaining a superficial understanding of what that really means for their companies. Corporate directors now must consider themselves on notice. When it comes to cybersecurity, they are expected to dig in and, therefore, must demand greater visibility into what is often presented as a murky and highly complex area best left to technologists.

Specifically, the 2018 SEC guidance advises that public companies should disclose the role of boards of directors in cyber risk management, at least where cyber risks are material to a company's business. With respect to the Google+ vulnerability, the SEC enforcement staff will probe about communication lines up to the board from the ground level at Google, searching for any broken links, any lack of transparency or candor, any concealment or "cleansing" of inculpatory information, and any other related corporate governance failure.

Historically, when it comes to their chief financial officers and the financial reporting function, the successful board paradigm has been one of vigorous and independent supervision, requiring the participation of independent third parties. The same should go for chief technology officers, chief information officers and chief information security officers, and the maxim of trust but verify should be equally operative in both contexts.

The SEC enforcement staff will want to know what steps, if any, Google took to enhance its board's cybersecurity oversight in response to the 2018 guidance, and will want to understand the

Google board's approach to cybersecurity and the Google board's involvement in the handling and management of the Google+ API defect.

3. Where was Google's CEO?

If Google's CEO does not embrace and understand the importance of cybersecurity, the company has little chance of effectively carrying out its responsibility to ensure proper risk-based measures are in place and functioning. It is the CEO who is charged with day-to-day management responsibility and, as history tells us, those in the organization will, in fact, "follow the leader." This may seem like an obvious point, but its criticality cannot be overstated.

Why would a CEO not take the issue of cybersecurity seriously? CEOs have a lot on their plate. And, like it or not, it is a reality of human behavior that there is a tendency to downplay the potential for certain risks — "this is not going to happen to us" — until those risks manifest themselves and then it is just too late. By then, the damage is already done, and the consequences can be immediate and, at times, catastrophic.

Recognizing this reality, the 2018 SEC guidance actually offers shareholders an assist in the effort to focus the attention of the CEO. The SEC explicitly recognizes the importance of "tone at the top," as demonstrated by one of its more specific and impactful directives, requiring that so-called executive certifications regarding the design and effectiveness of disclosure controls now encompass cybersecurity matters (such as certifications made pursuant to the Exchange Act Rules 13a-14 and 15d-14 as well as Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F).

Disclosure controls and procedures should ensure that relevant cybersecurity risk and incident information is reported to management so that they may make required certifications and disclosure decisions. Here, the SEC actually stole a page from the playbook of its former chairman, Harvey Pitt, who originated the idea of executive certifications way back in 2002.

Shocked after officials of such scandal-plagued companies as Enron and WorldCom testified on Capitol Hill that they did not know their companies were reporting false or misleading information, Pitt conjured up the idea of executive certifications, which was remarkably successful, effective — and quite ingenuous. Pitt dictated that top corporate officials, chief executive officers and chief financial officers, must declare personally — literally, to take an oath — that their most recent financial statements are accurate. The new rule applied to companies' future reports as well. By making a "certification," these officers are swearing that they know, for certain, that financial reports are true. If the reports are not, the executives must explain why these results are not accurate. This eventually led some companies to restate their results to comply with certification.

Just like Pitt's certification requirement sought to ensure accurate financial reporting and responsible executive conduct regarding financial results, current SEC Chairman Jay Clayton's 2018 SEC guidance seeks to ensure accurate cybersecurity reporting and responsible executive conduct regarding data security incidents.

These required certifications by a company's principal executive officer and principal financial officer as to the design and effectiveness of cyber-related disclosure controls and procedures can be somewhat challenging. Company executives making these certifications have to consider whether a company's disclosure controls and procedures for cybersecurity are, in particular, capable of fully assessing and escalating such cyber risks and incidents. Along these lines, the SEC will look to see if Google executives have developed and implemented some methodology to "drill down" into Google's technical conclusions, perhaps even independently validating information technology conclusions and representations when necessary.

The expanded certification rule seeks to drive executive-level ownership and accountability with respect to the reporting of cybersecurity incidents and the broader area of data security. Indeed, the 2018 SEC guidance states, "These certifications and disclosures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact."

The SEC certainly understands the centrality of the CEO's role, and now the CEO must affirmatively certify to the adequacy of the organization's cybersecurity controls. SEC enforcement

affirmatively certify to the adequacy of the organization's cybersecurity controls. SEC enforcement staff will attempt to determine if Google's CEO and senior executives have accepted — and embraced — both the spirit and the language of this new SEC certification requirement.

4. What were Google's formal policies, practices and procedures relating to disclosure of data security incidents?

SEC enforcement staff will want to review all of Google's formal policies, practices and procedures relating to the disclosure of cybersecurity incidents.

The 2018 SEC guidance encourages companies to implement policies, practices and procedures mandating that important cyber risk and incident information escalate "up the chain," from IT teams to senior management, allowing for informed, intelligent and knowledgeable decisions.

This particular communications edict must have hit close to home for Clayton, who, when testifying before Congress about a data breach at the SEC, was clearly miffed that the SEC staff had not shared certain critical information with the various SEC commissioners, including the chairman. At that time, then-SEC Commissioner Michael S. Piwowar even went so far as to issue a formal statement about the lack of communication to him about the SEC data breach, stating:

> I commend Chairman Clayton for initiating an assessment of the SEC's internal cybersecurity risk profile and approach to cybersecurity from a regulatory perspective. In connection with that review, I was recently informed for the first time that an intrusion occurred in 2016 in the SEC's Electronic Data Gathering, Analysis, and Retrieval ("EDGAR") system. I fully support Chairman Clayton and Commission staff in their efforts to conduct a comprehensive investigation to understand the full scope of the intrusion and how to better manage cybersecurity risks related to the SEC's operations.

5. What was the nature of any Google disclosure related to the data security incident or the risks of data security incidents?

Much like the 2011 SEC CF guidance, the 2018 SEC guidance can be somewhat maddening with respect to the actual content of a company's disclosure regarding a data security incident.

For example, as to the particularity of any data security incident's disclosure, the SEC seems to want to have its cake and eat it too. On the one hand, the 2018 guidance appears to allow for a lack of specifics so as not to compromise a company's security, stating:

> This guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts — for example, by providing a "roadmap" for those who seek to penetrate a company's security protections. We do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident.

On the other hand, the 2018 guidance cautions companies not to use any sort of generic "boilerplate" type of language in its disclosures, stating somewhat opaquely:

> We expect companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents. As the Commission has previously stated, we "emphasize a company-by-company approach [to disclosure] that allows relevant and material information to be disseminated to investors without boilerplate language or static requirements while preserving completeness and comparability of information across companies." Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.

Along these lines, any conclusions about the adequacy (or inadequacy) of the actual substance of any Google disclosure concerning the Google+ API defect will be the subject of debate. SEC staff will review texts, emails, reports and other relevant documents pertaining to the Google+ vulnerability discovery and remediation, and then follow up seeking testimonial evidence from Google employees and outside experts to better understand the particulars of the "bug."

With respect to Google's risk disclosures, the SEC enforcement staff will likely consider Google's vague reference to risk in its Oct. 8 announcement, which stated:

> The review did highlight the significant challenges in creating and maintaining a successful Google+ that meets consumers' expectations. Given these challenges and the very low usage of the consumer version of Google+, we decided to sunset the consumer version of Google+.

The SEC staff will want to know if Google incorporated into its SEC filings the risk associated with the "challenges," and will want to read the details of the Google "review," cited above in Google's Oct. 8 announcement.

***

This concludes part one of this two-part series. Please be sure and read part two, which will discuss: (1) the remaining five general questions that Google will likely have to answer if the SEC investigates, and (2) some final thoughts on what lies ahead for Google.

John Reed Stark is the president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as the chief of its Office of Internet Enforcement. He is the author of "The Cybersecurity Due Diligence Handbook."